大 韓 工 業 敎 育 學 會 誌
第 32卷 第 1 號 pp. 134-152

인터넷을 이용한 수업에서 패킷캡쳐를 통한 사이트 접속 제한

이 중 철* · 이 용 진**

<국문초록>

본 연구는 인터넷을 이용한 수업에서 학생들이 수업과 관련되지 않은 웹 사이트에 접속하는 것을 교사용 컴퓨터에서 발견하여 차단함으로써 수업의 효율성을 높이고, 교사가 의도하는 방향으로 수업을 진행할 수 있는 프로그램의 개발에 목적이 있다.

본 연구의 결과를 이용하면 수업과 관련되지 않은 웹 사이트에 접속하는 것을 방지하기 위하여 랜(LAN) 전원을 차단하고 수업하는 기존의 방법 대신 교수 매체로서 인터넷을 효과적이고 안전하게 사용할 수 있다. 관련 연구는 한 개의 호스트(host)만 감시하고 접속을 차단하는 반면에 본 연구에서 개발한 프로그램은 접속해 있는 모든 호스트들을 감시하고 차단할 수 있다.

본 연구에서 제안한 프로그램은 소규모 네트워크 환경에 설치된 리눅스(linux) 운영체제에서 개발되었다. 개발된 프로그램은 5가지 기능을 포함하고 있다. 도메인 네임(domain name)에서 IP(internet protocol) 주소로 변환하여 파일로 저장하는 변환기능, 인터넷을 사용할 준비가 되어 있는 학생 컴퓨터를 탐색하여 파일로 저장하는 탐색기능, 패킷(packet)을 캡쳐(capture)하여 패킷의 정보를 표현해주는 패킷 캡쳐 기능, 캡쳐된 패킷 정보와 차단 목록 데이터를 비교하는 비교기능, 그리고 차단 목록과 캡쳐된 패킷 정보가 일치할 경우 네트워크 접속을 차단하는 기능으로 구성되어 있다. 개발된 프로그램을 사용하면 네트워크를 통과하는 모든 패킷(packet)을 실시간에 정확하게 캡쳐 할 수 있고, 불량 사이트에 학생이 접근하는 경우 교사의 컴퓨터 화면에 관련 내용이 표시된다. 따라서 교사는 관련 내용을 실시간으로 확인하고, 불량 사이트에 대한 접속을 차단할 수 있다.

본 연구에서 개발된 프로그램은 초·중등학교와 같은 소규모 네트워크에 적용가능하며, 교사와 학생, 학교차원의 수업 관리와 컴퓨터 실습실 관리의 효율성을 향상시킬 것이다.

주제어 : 인터넷을 활용한 수업, 패킷 캡쳐, 실시간 모니터링, 접속 차단

* 교신저자, 이메일(bradnen0114@naver.com), 한국교원대학교 석사과정
** 한국교원대학교 교수

I. 서론

1. 문제 제기

통신기술의 발달, 보급과 확장은 정보 이동의 유용성과 양을 비약적으로 증가시켰다. 통신기술의 대표적인 매체는 단연 컴퓨터이다. 컴퓨터를 통해 알지 못하는 장소에 간접적으로 접근 하는 것이 쉬워졌으며, '정보화 시대'의 도래를 통해서 컴퓨터 활용은 모든 국가 체제의 기반 분야로 자리 잡게 되었다.

정보화 시대를 맞이하여 교육부는'교육정보화'를 목표로 '97년부터 각 학교에 컴퓨터를 비롯한 멀티미디어 설비를 보급하고 있다(문명환, 2000, p. 3). 이에 따라서 다양한 매체들이 교실 환경에 도입되면서 수업 환경이 달라지고 있다. 즉, 이제는 인터넷을 통해서 교사와 학생들이 교실 밖의 다른 교사, 학생, 전문가, 데이터베이스 및 다양한 프로그램들과 얼마든지 상호 작용할 수 있게 되었다(한국교육개발원, 1999, p. 6).

그러나 학교의 네트워크 환경에 있는 많은 컴퓨터들이 어떻게 네트워크에 참여중인지, 불량사이트 접근 시 경고 메시지 전송 등 중앙 컴퓨터에서 관리할 수 있는 네트워크 시스템이 없고, 수업시간에 게임, 인터넷 검색, 채팅 등을 사용하고 있는 컴퓨터에 대한 감시와 관리 시스템이 미비하다. 교사는 학생의 수업과 관련되어 있지 않은 행위를 모니터링 할 수 없으며, 방지하기 위해서 랜(LAN)의 전원을 차단하고 수업하는 경우가 있다. 또한 접속 현황을 보기 위해서 데이터를 관리 업체에 문의하는 불편함이 있다. 이런 현상들을 방지하고 학교의 소규모 네트워크를 손쉽게 관리하기 위하여 패킷(packet)을 캡쳐(capture)하는 도구를 사용하여 네트워크를 실시간으로 확인한다. 이로써 학생들의 행위를 감시할 수 있으며, 교사가 의도하는 방향으로 수업을 진행하고 불량사이트 접속을 차단 해주며 학교 네트워크의 효율적 관리를 위해서 새로운 프로그램의 필요성이 현장에서는 증대 되고 있다.

2. 연구 목적

본 연구의 목적은 초·중등학교 수업에서 인터넷을 이용할 때, 학생들이 수업과 관련되어 있지 않은 웹 사이트를 접근하는 것을 교사용 컴퓨터에서 발견하여 차단함으로써 수업 효율성을 높이고, 교사가 의도하는 방향으로 수업을 진행 하는 것이다. 또한 학생들의 수업 외 시간에 컴퓨터 사용에서는 불건전 사이트의 접속을 미리 차단하는 효과를 발휘하는 것이다.

3. 연구 내용

차단 목록에 있는 사이트의 접속을 차단하여 수업 시간에 수업과 관련되지 않은 사이트의 접속을 차단하고, 수업 외 시간에서는 불건전 사이트의 접근을 차단하는 프로그램의 개발하여 수업 효율성 증대를 위해서 세부적인 연구 내용은 다음과 같다.

첫째, 인터넷을 활용한 수업을 분석하여 장점과 단점을 도출한다.

둘째, 패킷과 패킷 캡쳐에 대해 알아본다.

셋째, 일반적인 사이트의 차단 방식을 분석한다.

넷째, 개발된 프로그램을 구현 환경에 적용하고 성능을 확인한다.

II. 이론적 배경

1. 선행 연구

윤치영, 정천복, 황선명(2001)은 실시간 네트워크 감시 시스템(Net Cop)을 구현 하였다. 호스트(host) 및 네트워크 사용을 원격에서 감시 및 제어를 함으로써 교수-학습의 편리를 위해 제공된 컴퓨터를 실시간으로 감시, 제어 및 관리를 할 수 있는 기능의 프로그램을 개발하였다. 그러나 한 번에 하나의 호스트 화면만 모니터링 하여 여러 호스트들에 적용을 할 수 없는 문제점이 있으며, 계속적인 실시간 모니터링으로 네트워크에 부담을 증가시키고, 작동 프로세스를 표시해줌으로써 관리자가 알아보는데 어려움이 있다.

반면 본 연구는 상용화된 차단 프로그램들의 기능을 수행하면서, 하나의 호스트가 아닌 소규모 네트워크 전체의 컴퓨터를 교사용 컴퓨터에서 실시간적으로 모니터링이 가능하고 원격지에서 불량사이트 접속을 차단할 수 있다.

2. 인터넷 활용 수업

컴퓨터를 포함한 다양한 매체들이 교실 환경에 도입 되면서 수업 환경이 달라지고 있다. 이에 따라서 전통적인 수업 방식에서 교사는 단순히 학습 내용을 전달하는 역할에서 고도의 정보 관리자, 그리고 학습 조력자 역할을 수행하며, 학습자는 전달되는 지식을 무조건 받아들이는 정보 수용자에서 자신이 부딪힌 문제를 해결하기 위해서

요구되는 지식을 결정, 탐색하는 능동적 학습자로 변화하고 있다(교육과정 평가원, 1998, pp. 6-7).

인터넷 활용 수업이란 말 그대로 인터넷을 수업에 활용하는 것이다. 인터넷을 수업에 활용하는 방법이나 목적, 형태 등은 다양하지만, 중요한 것은 인터넷 활용 수업 그 자체가 아니라 인터넷의 활용이 수업의 목적이나 수업의 질을 높이는 데 얼마나 도움을 줄 수 있느냐가 될 것이다(교육과정 평가원, 1998, p. 8).

가. 수업 유형

수업 도구로서 인터넷 활용 유형은 크게 두 가지로 나뉜다(교육과정 평가원, 1998, pp. 11-12).

첫째, 정보 차원의 보고인 인터넷을 자원기반 학습(resource-based learning)을 위한 도구로 활용하는 것이다. 많은 정보들 속에서 원하는 정보를 쉽게 얻을 수 있으며, 정보를 찾아가는 과정에서 문제해결 학습을 수행하는 것을 가능하게 한다.

둘째, 인터넷의 의사소통과 상호작용 지원 기능의 지원에 활용하는 것이다. 정해진 장소에서 교사가 전달하는 방식이 아닌 언제, 어디서든 교사나 또래 학습자들과 자료와 대화를 나누는 가운데 자율학습의 기틀을 마련할 수 있다.

나. 장점과 단점

인터넷을 활용한 수업에서 학습자는 고차원적 지적 능력을 개발할 수 있다. 다양하고 수많은 정보 속에서 적합한 정보를 찾기 위해 분석, 선별하는 활동을 수행하면서 스스로 정보의 의미와 가치를 창출하기 때문이다. 그리고 자기 주도적 학습 능력이 신장될 수 있다. 학습자가 스스로 학습 요구를 규명하여 학습상황을 통제하려는 책임감을 감당하고 학습목표에 도달하기 위한 적합한 학습 전략들을 적용한다. 관리자 입장에서 인터넷은 다양한 배경의 전문가들과 토론하므로 폭넓은 의견이나 관점을 나눌 수 있으며, 시간과 공간을 초월하기 때문에 융통성 있는 수업으로 진행이 가능해 진다(교육과정 평가원, 1998, pp. 24-26).

단점으로는 학습자에게는 동기가 부족할 경우 중간에 학습을 그만 둘 우려가 있으며, 수업 중에는 인터넷을 개인적인 일로 사용하는 일이 증대된다. 이 때문에 수업에 효율성이 저하된다. 또한 교사나 다른 학습자들과의 의사소통이 감소하므로 자신이 말 하고자 하는 바를 제대로 표현하는 능력이 저하된다. 관리자에게는 새로운 교수 방법과 절차를 익히는데 많은 노력이 필요하게 되며, 매체 활용에 대한 교사 교육이 제대로 실행되지 않고 있다(교육과정 평가원, 1998, p. 27).

3. 패킷과 패킷 캡쳐

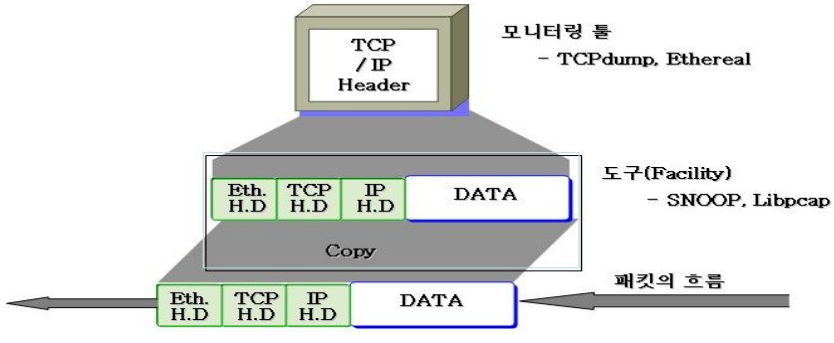
우리들이 현재 사용하는 통신은 다양한 통신망을 통해서 이루어진다. 현재 네트워크에서 정보의 전달이 이루어지는 방식은 패킷 교환(packet switching) 방식이다. 회선 교환(circuit switching)은 통신 자체가 안정적이기는 하나, 점차 늘어가는 환경을 감당하기 어려울 정도로 효율성이 낮고, 여러 가지 서비스를 제공하기 힘든 단점이 있다. 그래서 특정 전송로를 할당할 필요가 없는 패킷 교환 방식이 현재의 모든 네트워크 정보 송・수신 방식이 되었다.

패킷이란 통신과 네트워크에서 한 번에 전송되는 정보의 단위, 데이터의 한 블록(block)을 말하는 것이다(Kurose, 2005, p. 40). 즉, 현재 네트워크에서는 어떠한 종류의 파일이라도 파일을 전송하기에 알맞은 크기로 분할된다. 분할된 각 패킷들에는 별도의 순서 번호(sequence number)가 붙여지고, 적절한 경로를 찾아서 목적지에 도달하기 위한 최소한의 주소정보가 포함되며, 적절한 링크(link)를 통해서 전송한다.

김화종(2004)은 패킷 캡쳐를 네트워크를 통해 도착한 패킷을 읽은 작업이라고 정의하고 있다(p. 317). 또 다른 정의로 무라야마 유키오(2005)는 네트워크 내부를 흐르는 패킷을 들여다보는 것을 패킷 캡쳐 혹은 패킷 모니터링이라 부르고 있다. 패킷 캡쳐는 자신의 호스트 앞에 이르는 패킷이나 어느 곳에나 전달이 되는 브로드캐스트(broadcast) 패킷뿐만 아니라 다른 호스트 앞에 이르는 패킷도 들여다보는 것이 가능하다(p. 172).

패킷 캡쳐를 하기 위해서는 스누프(SNOOP), Libpcap과 같은 패킷 캡쳐 도구(facility)와 TCPdump, Ethereal 과 같은 패킷 모니터링 툴(tool) 혹은 스니퍼(sniffer) 가 있어야 한다. 패킷을 캡쳐하는 것은 지나가는 패킷을 잡아내는 것이 아니고, 패킷 캡쳐 도구에 의해서 패킷이 지나가는 순간에 똑같이 복사를 해서 모니터링 할 수 있는 툴로 보내주며, 모니터링 툴에 의해 패킷 정보를 확인할 수 있도록 화면에 출력을 해준다(www.kldp.or/Translations/Raw_IP_FAQ).

[그림 1]은 패킷을 캡쳐하는 개념도 이다.



[그림 1] 패킷 캡쳐 개념도

패킷 캡쳐는 네트워크를 운용하는 사람에게 네트워크의 설정 상태가 올바른지를 체크하거나 장애가 발생할 경우에 문제를 해결하거나 원인을 알아내는 데 도움이 된다. 또 네트워크 애플리케이션을 작성할 때에도 애플리케이션(application)의 동작과 패킷의 흐름을 관찰하면 프로그램을 조정하는 것이 가능하고 전송의 규약인 프로토콜(protocol)의 동작을 공부할 수 있다. 게다가 보안 향상을 위해서 네트워크에 부정 침입, 스캔 행위를 검출하거나 서비스 거부 (DOS - denial of service) 공격 등의 부정 패킷이 흐르는지를 검출할 수 있다. 패킷 캡쳐는 네트워크를 바르게 운용하기 위해서 사용되고, 네트워크 안을 흐르는 패킷은 모든 장치들이 케이블에 의해서 연결되어 있고 근거리 통신망 기술인 이더넷(ethernet)의 헤더(header)에서 애플리케이션의 메시지까지 볼 수 있다(무라야마 야키오, 2005, p. 172)

4. 유해 사이트 차단 방식

유해 사이트를 차단하는 방식은 <표 1>과 같다.

<표 1> 유해 사이트 차단 방식의 분류

차단 방법에 따른 분류	차단 목록 기반의 선별 기술
	허용 목록 기반의 선별 기술
	내용 등급 기반의 선별 기술
적용 범위에 따른 분류	인터넷 접속 단말기에서의 차단
	인터넷 접속 관문에서의 차단

차단 목록 기반의 선별 기술은 차단 대상 URL(uniform resource locator)을 저장하고 있는 데이터베이스를 만들어 접근을 차단하는 방식이다. 사이트 주소가 데이터베이스에 있을 경우에는 접속을 허용하지 않게 하는 기술이다. 국내 대부분의 차단 프로그램이 이 방식을 사용하고 있다(심재권 외 2 인, 2000, p. 639; 김재천, 2001, p. 30).

허용 목록 기반 선별 기술은 내용이 검증되어 데이터베이스에 등록된 사이트만 접근을 허용하고 이외의 사이트는 모두 차단하는 방식이다(심재권 외 2 인, 2000, p. 639; 김재천, 2001, p. 31).

내용 등급 기반 선별 기술은 일정 기준에 의해 정의된 등급에 의해 차단된다. 등급은 인터넷 내용 선별 기술 체계(PICS : platform for internet contents selection)에 의해 분류된다. 단점은 하나의 컴퓨터를 여러 명이 사용할 때 연령별로 차단 수준을 다르게 할 수 없는 문제를 안고 있다(심재권 외 2 인, 2000, p. 639; 김재천, 2001, p. 31).

인터넷 접속 단말기에서 차단은 브라우저(browser)가 설치된 컴퓨터의 인터넷 접속 단말기에서 차단하는 방법으로 가정 등 소규모 네트워크에서 사용이 편하다. 단점은 인터넷 접속이 가능한 모든 단말기에 차단 프로그램을 설치하여야 한다(심재권 외 2인, 2000, p. 639; 김재천, 2001, p. 33).

인터넷 접속 관문에서 차단은 게이트웨이(gateway)나 프락시 서버(proxy server) 등의 인터넷 접속 관문에서 차단 프로그램을 설치하여 네트워크 관리자가 차단 규칙을 설정하여 관리한다. 기업이나 학교, ISP(internet service provider) 등 대규모 집단에서 사용이 편리하다. 단점은 모든 사용자가 동일한 차단 규칙에 적용이 된다(심재권 외 2인, 2000, p. 639; 김재천, 2001, p. 33).

현재 프로그램으로 사용되고 있는 보편적인 차단 기술은 차단 목록 기반 선별 기술이며, 국내 및 외국의 대다수 인터넷 불건전 정보 차단 프로그램이 이 기술을 사용하고 있다. 본 연구에서의 차단 방식도 차단 목록 기반 방식을 사용할 것이다.

5. TCP 접속차단 원리

TCP(transmission control protocol)연결에서 접속을 차단하는 원리 이해하기 위해서는 TCP 헤더와 IP(internet protocol) 헤더를 사전에 알고 있어야 한다. TCP 헤더와 IP 헤더를 설명하는 부분은 많이 다른 자료에서도 많이 언급되어 있으므로 생략하고, 본 연구에서는 특별히 플래그(flag)라는 필드에 대한 이해를 다룬다. 플래그는 제어 플래그라고 불리우며, <표 2>는 TCP의 헤더에 들어있는 플래그를 설명한 것이다.

<표 2> TCP 헤더에서 각각의 제어 플래그의 의미

플 래 그	값	비트가 [1]일 경우 의미
URG(urgent flag)	0x20	이동하고 있는 데이터 중에 긴급히 처리해야 하는 것이 포함되어 있는지 아닌지를 의미한다. 긴급히 처리해야 하는 데이터는 긴급 포인터의 필드에 나타난다.
ACK(acknowledgement flag)	0x10	확인 응답 필드가 유요한 것을 의미한다. 가장 최초의 SYN 세그먼트 이외는 반드시 [1]로 되어있다.
PSH(push flag)	0x08	송신한 데이터를 지연되지 않게 신속히 애플리케이션에 전해 주도록 지원한다.
RST(reset flag)	0x04	연결을 강제적으로 차단하는 것을 의미한다.
SYN(synchronize flag)	0x02	연결 요구를 의미한다. 순서번호 필드의 값을 순서번호의 초기값으로 한다.
FIN(fin flag)	0x01	연결 차단 요구를 의미한다. 통신의 마지막 세그먼트에 있는 것을 의미하고 이 세그먼트 외에는 데이터 세그먼트가 송신되지 않는다.

이중에 눈여겨봐야 할 플래그가 바로 RST 플래그 이다. RST 플래그는 비정상적으로 연결을 종료해야 할 때 상대방 호스트에 전송하는데 사용되는 플래그로 TCP 연결이 갑자기 끊어질 때 주로 시스템(운영체제) 차원에서 많이 사용하는 플래그이다. RST 플래그는 상대방으로부터의 연결시도에 대해 거절(deny)하는 경우에도 사용되지만, 연결이 이루어져 한창 통신하는 도중에도 사용될 수 있다. 본 연구에서는 선생님 컴퓨터에서 학생 컴퓨터로 RST 플래그가 설정된 패킷을 송신하면 학생 컴퓨터는 차단 사이트와의 연결이 끊어진 것으로 착각을 하고 이후 차단 사이트의 서버로부터 요청되는 TCP 통신에 대해서는 전부 거절하게 된다. 이러한 방식으로 연결이 자동적으로 끊어지게 된다.

III. 연구 방법

1. 연구 목표

본 연구에서는 실시간으로 네트워크의 모든 호스트들을 모니터링하고, 수업과 관련되어 있지 않은 사이트 접근을 차단하여, 교사와 학생에게 효율적인 학습 환경을 제공하기 위한 시스템으로 다음과 같은 목표를 두고 개발하고자 한다.

첫째, 관리자가 쉽게 사용할 수 있는 사용자 인터페이스(interface)를 제공해야 한다.

둘째, 실시간 모니터링과 간단한 제어 기능의 상호연동이 유연하게 이루어져야 한다.

셋째, 정확한 네트워크 모니터링 기능을 제공하여야 한다.

넷째, 패킷 정보를 파일에 정확하게 작성이 되어야 한다.

넷째, 오랜 시간동안 사용해도 시스템에 부하가 적어야하고 오류가 없어야 한다.

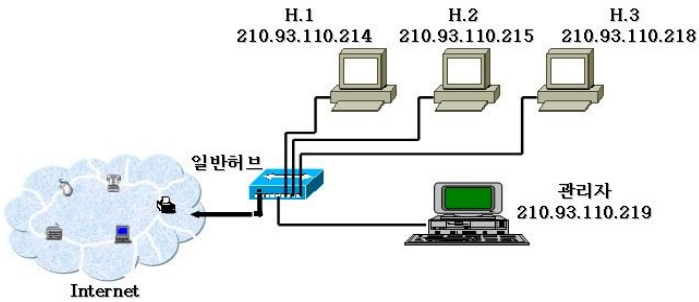
2. 연구 환경

본 연구에서 1개의 관리자 컴퓨터(교사용 컴퓨터)와 3개의 호스트 컴퓨터(학생용 컴퓨터)의 총 4대의 컴퓨터로 구성된 소규모 네트워크 환경이다. 컴퓨터들은 일반 허브(dummy hub)에 의해서 서로 연결이 되어 있다. 각 컴퓨터의 시스템 사양은 <표 3>과 같으며, 연구 환경은 [그림 2]과 같다.

<표 3> 시스템 사양

구 분	IP 주소	내 용	
관 리 자	210.93.110.219	하드웨어	펜티엄 듀얼 3.4G 1.28G RAM 300G H/D
		운영체제	Linux Ubuntu(커널2. 6. 15)
호스트 1 (H.1)	210.93.110.214	하드웨어	Intel Xeon(TM) 3.0G 1.28G RAM 80G H/D
		운영체제	Linux Fedora(커널2. 6. 20)
호스트 2 (H.2)	210.93.110.215	하드웨어	펜티엄 4 2.4G 1.28G RAM 40G H/D
		운영체제	Linux Ubuntu(커널2. 6. 15)
호스트 3 (H.3)	210.93.110.218	하드웨어	펜티엄 4 1.4G 512M RAM 120G H/D
		운영체제	Linux Ubuntu(커널2. 6. 15)

<표 3>의 시스템 사양에서 운영체제는 리눅스 우분투(ubuntu)와 페도라(fedora)를 사용하고 있으며 이들에 대한 각각의 IP 주소도 함께 제시하였다. 관리자 컴퓨터는 시스템 부하를 고려하여 성능이 가장 좋은 컴퓨터로 선정했다.



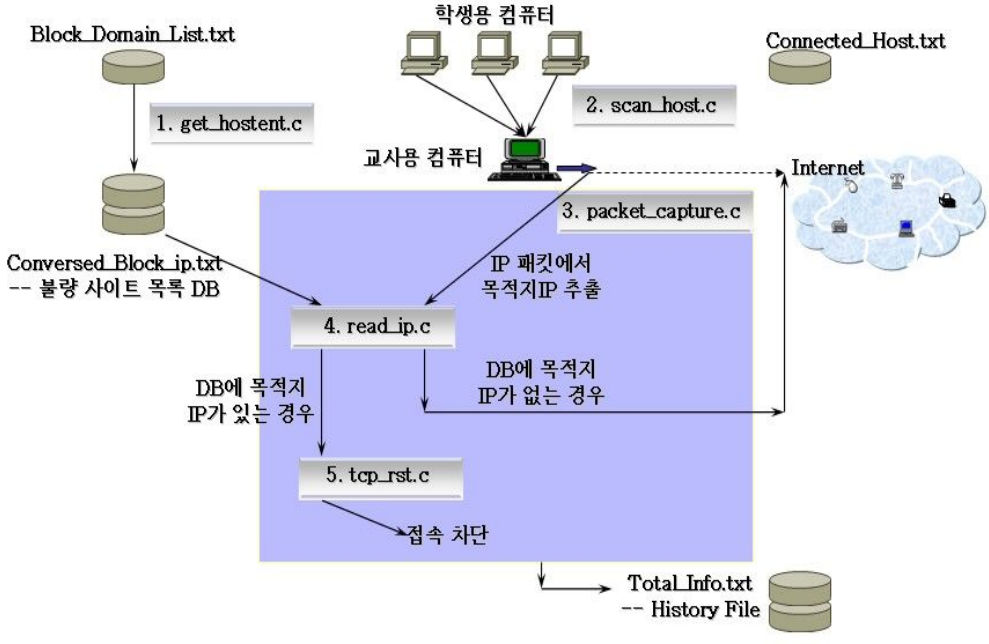
[그림 2] 연구 환경

[그림 2]의 연구 환경을 보면 인터넷으로 연결되기 전에 일반 허브에 의해서 모든 컴퓨터가 연결되어 있는 것을 확인 할 수 있다. 일반허브에서는 패킷이 연결되어 있는 모든 호스트에 전달이 되는 특성(broadcast)이 있어서 관리자 컴퓨터에서 네트워크의 모든 호스트를 향하는 패킷을 캡쳐할 수 있다.

3. 시스템의 설계 (기능별 구분)

[그림 3]은 본 연구에서 개발한 프로그램의 체계적인 과정을 나타낸 것이다. 이를 기능별로 구분하면 다음과 같다.

- 도메인 네임(domain name)에서 IP 변환 기능(1. get_hostent.c) :
  도메인 네임을 도메인 네임 + IP 주소 형태의 데이터베이스로의 전환
- 접속 호스트의 탐색 기능(2. scan_host.c) :
  인터넷을 사용할 준비가 되어 있는 호스트 탐색
- 패킷의 캡쳐 기능(3. packet_capture.c) :
  Libpcap을 이용(C언어), 실시간 패킷 모니터링, 프로토콜의 분석
- 목적지 IP와 데이터베이스의 비교 기능(4. read_ip.c) :
  접속의 차단에 관한 결정을 위한 비교
- 접속 차단 기능(5. tcp_rst.c) :
  차단 목록과 캡쳐된 패킷의 목적지 IP가 일치하는 경우 차단 실행



[그림 3] 시스템의 과정

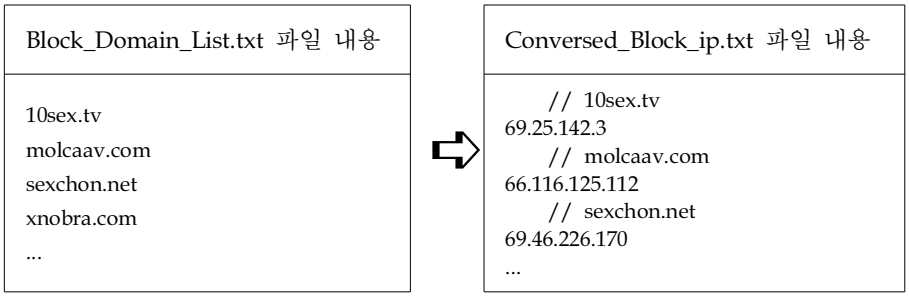
[그림 3]에서 나타낸 기능들은 각각의 프로그램이 작동하는 것을 의미하며, 프로그램들은 상호 연결 관계를 갖고 있고 하나의 명령어에 의해서 모든 프로그램들이 컴파일 되도록 make 유틸리티를 사용해서 사용자가 쉽게 프로그램을 다룰 수 있다. 프로그램들의 실행과정과 생성되는 파일의 설명은 다음 장에서 언급하도록 한다.

IV. 연구 결과

본 연구에서 개발된 프로그램들은 구현된 소규모 네트워크에서 리눅스 운영체제에서 개발되었다. 프로그램을 실행하기 위해서는 명령을 실행할 수 있는 터미널(terminal) 창에서 실행하여야 한다. 화면에 나타나는'hjung/cheol'은 사용 프로그램들이 들어있는 폴더의 경로를 나타내며 '#'은 사용자가 루트(root)상태임을 나타내는 프롬프트(prompt)이다. 그림들에서 키보드로 직접 관리자가 입력하는 경우에는 음영(陰影)을 주고, 프로그램이 실행하면서 자동적으로 나타나게 되는 표준출력과의 구별을 용이하게 하였다. 리눅스에서 명령어를 실행할 때에는 항상 './명령어'를 해주어야 함을 주의하여야 한다.

1. 도메인 네임에서 IP 주소 변환 프로그램 (get_hostent.c)

프로그램 파일명 get_hostent.c는 웹의 주소를 쉽게 알아볼 수 있는 도메인 네임을 점십진법의 형태 IP 주소로 바꿔주는 프로그램이다. 사이트를 접속할 때 도메인 네임이 아닌 IP 주소로 접속이 이루어지기 때문에 패킷을 캡쳐하면 IP 주소가 나온다. IP 주소로 변환해주는 이유는 캡쳐된 패킷의 목적지 IP 주소 정보와 차단 목록을 비교하여 이후에 차단 혹은 통과 결정을 하는데 사용된다. 이러한 이유로 IP 주소로 변환을 시켜주는 것이다. 도메인 네임 목록은 텍스트 파일의 Block_Domain_List.txt 로 저장이 되어 있으며, 텍스트 파일에서 한 줄씩 읽어 들여 IP 주소로 변환이 되어 도메인 네임과 IP 주소가 함께 Conversed_Block_ip.txt 파일에 저장 된다. [그림 4] 은 명령어 실행 후 파일 변화를 나타낸 그림이다.



[그림 4] 명령 실행 이후의 파일 변화

실행 명령어를 입력하면 Block_Domain_List.txt 파일 내용의 도메인 네임들이 IP 주

소와 함께 Conversed_Block_ip.txt에 저장 된다. 예를 들면, 'xnobra.com' 의 IP 주소는 '69.46.226.170'임을 알 수 있으며, 이들은 새로운 파일명에 함께 저장 된다.

2. 접속 호스트 탐색 프로그램 (scan_host.c)

프로그램 파일명 scan_host.c는 인터넷에 연결할 수 있는 지 확인하는 핑(ping : packet internet proper)을 호스트들에게 전송하여 응답이 오는 경우에 이를 Connected_Host.txt 에 저장하는 프로그램이다. 절차는 탐색시작 호스트 IP 주소와 종료하는 IP 주소를 지정해주고, 지정한 범위의 IP 주소가 설정된 호스트가 존재하는지의 여부를 ICMP(internet control message protocol) 에코요구(echo request)패킷을 사용하여 검색을 한다. 에코요구 패킷은 해당 호스트가 존재하면 응답을 해달라는 요청을 하는 패킷이다. 저장되는 파일은 패킷을 캡쳐한 후에 근원지 IP 주소 정보가 검색된 호스트의 IP 주소와 동일한지 비교하는데 사용된다.

[그림 5]는 호스트 탐색 명령어를 실행 후 화면과 생성된 파일 내용이다.

명령 실행 후 교사 컴퓨터 화면	Connected_Host.txt 파일 내용
hjung/cheol# **./sh** Input Start IP : **210.93.110.211** Input Last IP : **210.93.110.218** Host Scanning... 1 : 210.93.110.214 : RTT= 0.6590ms 2 : 210.93.110.215 : RTT= 2.6606ms 3 : 210.93.110.218 : RTT= 0.6340ms Total Host is 3 ... hjung/cheol#	210.93.110.214 210.93.110.215 210.93.110.218 // Total host is 3 ...

[그림 5] 명령 실행 후 화면과 파일 내용

교사가 처음 시작할 때 인터넷 사용 준비된 학생들의 컴퓨터를 찾기 위한 명령어를 실행하고 검색을 시작하려는 IP 주소 '210.93.110.211'과 검색 종료지점의 IP 주소 '210.93.110.218'을 입력한다. 교사용 컴퓨터는 지정범위의 컴퓨터들을 자동으로 검색하고, 인터넷 사용 준비가 된 컴퓨터의 IP 주소를 보여주고 파일에 저장한다. 파일의 내용은 검색된 IP 주소만 검색된 순서대로 저장하고 총 검색된 컴퓨터의 수를 표시해 준다. 파일안의 IP 주소는 이후에 패킷을 캡쳐 하였을 경우 패킷이 포함하고 있는 근원지 주소정보와 비교시 활용 된다. RTT(round trip time)는 응답이 돌아오는데 걸린 시간을 의미하며 단위는 밀리세컨드(ms) = 1/1000 초이다.

3. 패킷 캡쳐 프로그램 (packet_capture.c)

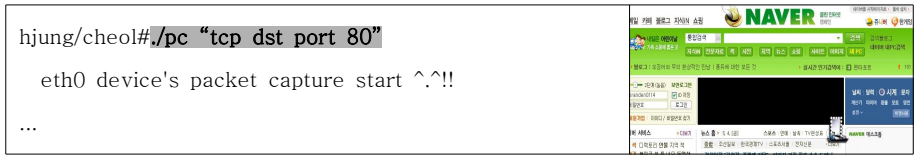
프로그램 파일명 packet_capture.c는 libpcap을 이용하여 네트워크를 지나가는 모든 패킷을 캡쳐 하도록 작성된 프로그램이다. 프로그램은 패킷을 캡쳐 했을 경우 목적지 IP 주소와 근원지 IP 주소를 추출하기 위해서 IP 헤더를, 목적지 접속 포트와 근원지 접속 포트를 알기 위해서 TCP 헤더를 분석한다. 분석된 정보는 Total_Info.txt 파일에 저장된다. 필터링 규칙은 Libpcap의 기본 API(application programming interface)에서 지원해 주는 규칙이 적용된다.

[그림 6]은 패킷 캡쳐 명령어와 옵션을 설정한 후 이를 실행한 화면이다.

```
hjung/cheol#./pc  "tcp dst port 80"
  eth0 device's packet capture start ^.^!!
```

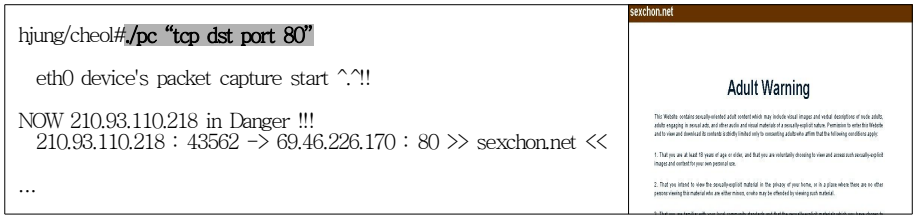
[그림 6] 명령 실행 후 교사의 컴퓨터 화면

'./pc'명령 실행 후 옵션을 "tcp dst port 80"으로 지정했다. 대부분의 웹은 80번 포트 번호를 이용해서 데이터들이 전송이 되므로 목적지의 포트번호가 80번인 패킷을 캡쳐 한다는 옵션을 지정해 준 화면이다. 그 후에 랜카드 장치 번호'eth0'를 통과하는 모든 패킷의 캡쳐가 시작된다는 메시지가 표준출력 된다.



[그림 7] 차단 목록에 들어있지 않은 사이트 방문시 교사의 컴퓨터 화면

[그림 7]은 패킷 캡쳐 명령어를 실행하고 차단 목록에 들어있지 않은 건전한 사이트를 접속했을 때 교사의 컴퓨터 화면을 나타낸다. 화면에는 패킷 캡쳐를 시작했을 때와 화면에서 차이가 없다. 이는 학생들의 컴퓨터가 차단 목록 사이트에 접속을 하고 있지 않다는 뜻이다.

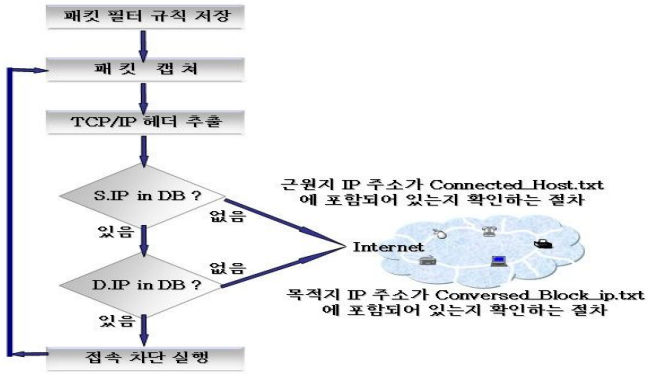


[그림 8] 차단 목록에 있는 사이트 방문시 교사의 컴퓨터 화면

[그림 8]은 차단 목록에 있는 사이트에 '210.93.110.218'의 IP 주소를 가진 학생의 컴퓨터가 '69.46.226.170'의 IP 주소를 가진 사이트에 접속 하고 있다. 이 사이트의 도메인 네임도 교사의 컴퓨터 화면에 자동적으로 출력이 된다. 또한 캡쳐된 정보(목적지 IP, 근원지 IP, 목적지 포트번호, 근원지 포트번호, 확인응답 번호)를 인자로 갖는 포인터 배열을 생성한다. 이 정보로 이루어진 포인터 배열은 차단 프로그램이 실행될 때 필요로 하는 요소들이며, 포인터 배열을 받은 차단 프로그램은 자동으로 실행되어 연결 종료가 된다. 그러므로 교사는 자신의 컴퓨터 화면을 보면 어떤 학생이 어디로 접속을 하는지 알 수 있고 즉각적인 경고를 줄 수 있다.

4. 목적지 IP와 DB의 비교 프로그램 (read_ip.c)

프로그램 파일명 read_ip.c는 패킷 캡쳐에 의해 추출된 목적지 IP 주소가 get_hostent.c에 의해서 실행된 차단 목록에 포함이 되어 있는지 판별하는 프로그램이다. 차단 목록에 있다면 수업과 연관되지 않은 사이트에 접속을 하고 있다는 증거이다. 비교 검색속도를 높이기 위해 해싱(hashing) 기법을 사용하였다. 해싱기법은 해시테이블(hash table)이라는 기억 공간을 할당하고, 해시함수를 이용하여 메모리에 블록 단위로 정보를 저장하고, 임의의 문자열을 빠르게 검색 위한 직접파일 구조이다.
[그림 9]는 근원지 IP 주소와 목적지 IP 주소를 차단 목록에서 검색하기 위한 순서도를 나타낸 그림이다.



[그림 9] IP 주소 검색 순서

[그림 9]에서 보듯이 1차 IP 주소 검색은 차단목록인 Connected_Host.txt 파일 안에 캡쳐된 패킷의 근원지 주소와 일치 하는지 확인 한 후, 파일 안에 들어 있을 경우에는 2차 IP 주소 검색이 시작된다. 목적지 IP 주소가 IP 주소와 도메인 네임이 함께 저장되어 있는 Conversed_Block_ip.txt 파일 안에 있는지 확인하고, 들어 있는 경우에는 교사의 컴퓨터 화면에 접속을 시도하려는 학생의 컴퓨터에 대한 경고의 메시지가 자동적으로 출력이 된다. 교사는 이를 즉시 확인 할 수 있으며 학생의 컴퓨터는 접속하려는 사이트와 연결이 종료된다.

5. 접속 차단 프로그램 (tcprst.c)

프로그램 파일명 tcprst.c 프로그램은 캡쳐된 패킷에서 목적지 IP 주소가 차단 목록에 포함이 되어 있는 경우에 작동되는 프로그램이다. 패킷 캡쳐 프로그램으로부터 포인터 배열로 작성된 정보들이 차단 프로그램을 작동하는 기본 정보이다. 선생님 컴퓨터로부터 학생 컴퓨터로 연결을 초기화 하는 TCP-RST(reset) 플래그 값이 설정되어 있는 세그먼트(segment) 패킷이 흐르게 되는데, 이는 TCP의 연결을 강제적으로 차단한다. 연결을 강제적으로 차단하는 것은 데이터 송·수신에 관한 신뢰성도 잃어버리게 된다. RST 세그먼트 패킷을 받은 학생 컴퓨터는 어떠한 정보도 보내지 않고 연결 정보를 초기화 하며, 이후 차단 사이트의 서버로부터 요청되는 TCP 통신에 대해서는 전부 거절하게 된다. 이러한 방식으로 연결이 자동적으로 끊어지며, 더 이상 두 호스트들 간에는 정보를 받아들일 수 없게 되고 연결이 종료가 된다.

6. 히스토리 파일 (Total_Info.txt)

Total_Info.txt 파일은 Connected_Host.txt 파일 안에 저장된 호스트에서 송·수신되

는 모든 패킷의 간략한 정보를 시간과 함께 저장한다. 저장된 파일은 일별/주별/월별 통계에 활용할 수 있으며, 학생들의 접속 현황을 파악할 수 있는 기초 자료로 활용이 가능하다. 이를 통해서 학생들이 수업 중에 자주 접근하는 사이트를 차단 목록에 교사가 임의적으로 추가하명 강력한 차단 기능을 수행할 수 있다. 더불어 차단 목록을 교사용과 학생용으로 개별적 적용할 수 있다. [그림 4 - 7]은 Total_Info.txt 파일 안의 내용이다.

```
Sat Apr 28 17:47:26 2007
  /  IP-Source  /     IP-Dest    /                  / S-Port / D-Port /
  210.93.110.218   222.122.84.250                      43502    80
...

Sat Apr 28 17:50:13 2007
  /  IP-Source  /     IP-Dest    /                  / S-Port / D-Port /
  210.93.110.218   69.46.226.170 >>Check Success<<  43562    80   Tcp_rst Start
...
```

[그림 10] Total_Info.txt 파일 내용

[그림 10]에서 보듯이 Total_Info.txt 파일 안의 첫줄은 패킷이 캡쳐된 시간이 표시된다. 그리고 정상적인 사이트에 접속 했을 때 패킷이 저장된 형태를 나타낸다. '210.93.110.218'의 IP를 가지고 있는 학생의 컴퓨터가 '222.122.84.250 (www.naver.com)'에 접속을 하였을 경우이다. 조금 후의 패킷은 같은 주소를 갖고 있는 컴퓨터가'69.46.226.170'의 IP 주소를 가지고 있는 사이트에 접속을 하였을 경우 저장된 패킷정보이다. 차단 목록에 목적지 IP 주소가 이미 저장이 되어 있기 때문에 검색이 되고, 검색이 되었다는 메시지로 "Check Success" 를 표시해준다. 후에 차단 프로그램이 자동적으로 실행되며, 실행 메시지를 "Tcp_rst Start"라고 표시하고 있다.

V. 요약 및 결론

본 연구는 인터넷을 수업에 활용함으로써 학생들의 수업과 관련되어 있지 않은 웹사이트를 방문하며, 수업의 효율성이 낮아지는 것을 방지하는 프로그램을 개발하는데 목적이 있다. 본 개발 프로그램을 사용하면, 랜 전원을 차단하고 수업 하는 기존의 방식 대신 교수 매체로서의 인터넷을 효과적이고 안전하게 사용할 수 있고, 교사가 의도하는 방향으로 수업을 진행할 수 있다. 관련연구에서는 한 개의 호스트만 감시하고 접속을 차단하는 반면에, 본 연구에서 개발한 프로그램은 접속해 있는 모든 호스트들을 감시하고 차단할 수 있다.

본 연구에서 제안한 프로그램은 소규모 네트워크를 통과하는 환경에 설치된 리눅스 운영체제에서 개발되었다. 개발된 프로그램은 각자의 프로그램이 상호 관계가 있도록 구현되었고, 네트워크를 통과하는 모든 패킷을 원활하게 캡쳐 할 수 있었으며, 불량 사이트에 학생이 접근하는 경우 교사의 컴퓨터 화면에 관련내용이 표시되었다. 따라서 교사는 관련 내용을 실시간으로 확인하고, 불량 사이트에 대한 접속을 차단하며 학생에 대해서 경고 메시지를 이야기할 수 있다.

개발된 프로그램을 소규모 네트워크에 적용할 경우에는 교사와 학생, 그리고 학교에서는 다음과 같은 효과를 기대할 수 있다.

첫째, 교사는 학생들의 수업과 연관되지 않은 웹 사이트의 접속이 실시간 모니터링 가능하다. 기존 프로그램은 학생들의 컴퓨터 개개인을 모니터링 할 수 없었다. 이에 반해 개발된 프로그램은 학생들의 행위에 대해 실시간 모니터링이 가능하고, 교사는 즉각적인 반응을 보일 수 있다.

둘째, 교사는 학생들의 웹 사이트 접속을 차단할 수 있다. 학생 컴퓨터의 접속이 자동적으로 차단되어 수업과 관련 없는 사이트의 접근이 감소하고, 수업과 관련 있는 컴퓨터의 사용이 이루어질 수 있다.

셋째, 학교에서는 차단 방식의 개별화를 적용할 수 있다. 기존 차단 프로그램에서는 교무실 컴퓨터들과 실습실 컴퓨터를 구분하지 않고, 모든 접근을 차단하였다. 그러나 개발된 프로그램은 차단의 설정을 다르게 할 수 있다.

향후 연구에서는 실제 학교 현장에 적용하여 수업을 분석하는 연구가 필요하며, 스위칭 허브(switching hub) 환경에서도 적용 가능한 프로그램의 개발이 기대되고, 아울러 동시접속환경에 대한 프로그램 차단 성능 측정 개량화를 통한 성능 평가가 기대된다.

참 고 문 헌

교육과정평가원(1998). 인터넷을 이용한 수업개선 연구. 교육과정평가원.

김재천(2001). 인터넷 유해 사이트 차단 프로그램 분석 및 활용방안. 석사학위 논문. 홍익대학교.

김화종(2004). 컴퓨터 네트워크 프로그래밍. 홍릉과학출판사.

문명환(2000). 네트워크 환경에서의 학교 컴퓨터의 관리 방안. 석사학위 논문. 경상대학교.

심재권, 김귀복, 박기홍(2000). 유해정보의 경향과 유해 정보차단 소프트웨어의 문제점에 관한 연구. 한국정보과학회 학술발표논문집, **27**(2).

유호경, 한기희, 김철희(2001). 인터넷 불건전사이트 구축 시스템**(XRobot 1.0)** 개발 완료 보고서. 정보통신윤리위원회.

윤치영, 정천복, 황선명(2001). 실시간 네트웍 감시 시스템**(Net Cop)**의 설계 및 구현. 한국정보교육학회, **5**(3), 374-379.

이원준, 안상현, 최웅철(2004). 컴퓨터 네트워킹(인터넷 프로토콜 및 기술). ITC.

장대진 (2001).윈도우 기반의 패킷 분석 모듈의 설계 및 구현. 석사학위 논문. 계명대학교.

무라야마 유키오(2005). 기초부터 배우는 **TCP/IP**네트워크 실험 프로그래밍(송봉길 역). 성안당.

Craig Hunt(2000). TCP/IP 네트워크 관리. 한빛미디어.

James F. Kurose, Keith W. Ross(2005). 컴퓨터 네트워킹(3rd ed.), (강현국, 신용태, 안상현, 최종원 역). 피어슨에듀케이션코리아.

Williams Stallings(2001). 데이터 통신 및 컴퓨터 통신(김종상, 전화숙 역). 사이텍미디어.

http://tyranno.chonnam.ac.kr/lecture/2003_Fall/Doc/Introduction_libpcap.html

http://www.kldp.org/Translations/Raw_IP_FAQ

◎ 논문접수: 2007. 4. 30 / 1차수정본 접수: 2007. 6. 4 / 게재승인: 2007. 6. 12

<Abstract>

Access Restriction by Packet Capturing during the Internet based Class

Jungcheol, Yi* · Yong-Jin, Lee**

This study deals with the development of computer program which can restrict students to access to the unallowable web sites during the Internet based class. Our suggested program can find the student's access list to the unallowable sites, display it on the teacher's computer screen. Through the limitation of the student's access, teacher can enhance the efficiency of class and fulfill his educational purpose for the class.

The use of our results leads to the effective and safe utilization of the Internet as the teaching tools in the class. Meanwhile, the typical method is to turn off the LAN (Local Area Network) power in order to limit the student's access to the unallowable web sites.

Our program has been developed on the Linux operating systems in the small network environment. The program includes following five functions: the translation function to change the domain name into the IP(Internet Protocol) address, the search function to find the active students' computers, the packet snoop to capture the ongoing packets and investigate their contents, the comparison function to compare the captured packet contents with the predefined access restriction IP address list, and the restriction function to limit the network access when the destination IP address is equal to the IP address in the access restriction list.

Our program can capture all passing packets through the computer laboratory in real time and exactly. In addition, it provides teacher's computer screen with the all relation information of students' access to the unallowable sites. Thus, teacher can limit the student's unallowable access immediately.

The proposed program can be applied to the small network of the elementary, junior and senior high school. Our research results make a contribution toward the effective class management and the efficient computer laboratory management.

The related researches provides teacher with the packet observation and the access limitation for only one host, but our suggested program provides teacher with those for all active hosts.

Key words: Internet based class, packet capture, real-time monitoring, access restriction

---

* Correspondence, Graduate School of Korea National University of Education
** Korea National University of Education